DERWENT-ACC-NO:	1999-481196
DERWENT-WEEK:	200175

COPYRIGHT 2007 DERWENT INFORMATION LTD

TITLE:	Dynamic distribution of program objects
INVENTOR:	COHEN, G A; KAMINSKY, D L ; KING, R A
PATENT-ASSIGNEE:	INT BUSINESS MACHINES CORP [IBMC] , IBM CORP [IBMC]
PRIORITY-DATA:	1998US-0036270 (March 6, 1998)

PUB-NO	PUB-DATE	LANGUAGE	PAGES	MAIN-IPC
EP 940748 A2	September 8, 1999	E	021	G06F 009/46
US 6324543 B1	November 27, 2001	N/A	000	G06F 012/00
JP 11312088 A	November 9, 1999	N/A	017	G06F 009/44

DESIGNATED-STATES:	AL AT BE CH CY DE DK ES FI FR GB GR IE IT LI LT LU LV MC MK NL PT RO SE SI

APPLICATION-DATA:

PUB-NO	APPL-DESCRIPTOR	APPL-NO	APPL-DATE
EP 940748A2	N/A	1999EP-0301529	March 2, 1999
US 6324543B1	N/A	1998US-0036270	March 6, 1998
JP 11312088A	N/A	1999JP-0032596	February 10, 1999

INT-CL (IPC):	G06F009/44, G06F009/46 , G06F012/00 , G06F015/16 , G06F015/173

ABSTRACTED-PUB-NO:	EP 940748A

BASIC-ABSTRACT:

NOVELTY - Method consists in identifying all the objects in the program, creating a list of conditions under which objects of the program are to be migrated, and identifying each programmed entity to be accessed from outside of the object. Two proxies are generated for each object, one on the same physical device and the other transferred to the remote computer on object migration. The first proxy contains network linkage and indication to access the programmed entities on the remote computers, and the second contains network linkage and indication to access the programmed entities on the first computer.

EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	2	"6182275".pn.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/05/08 15:43
L2	2	"6,167,383".pn.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/05/08 15:43
L3	1	"6,167,383".pn. and http	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/05/08 15:45
L4	0	"6,167,383".pn. and (http with (content field))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/05/08 15:45
L5	895	(@ad<"20000410").ad. and (http) and (secure with (box computer machine))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/05/08 15:58
L6	430	(@ad<"20000410").ad. and (http) and (secure with (box computer machine)) and (select$5 same (component part feature))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/05/08 15:59
L7	380	(@ad<"20000410").ad. and (http) and (secure with (box computer machine)) and ((select$5 choos$5 determin$5 chos$5) with (component part feature))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/05/08 16:01
L8	380	(@ad<"20000410").ad. and (http) and (secure with (box computer machine)) and ((select$5 choos$5 determin$5 chos$5) with (component part feature))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/05/08 16:01
L9	111	(@ad<"20000410").ad. and (http) and (secure with (box computer machine)) and (((select$5 choos$5 determin$5 chos$5) with (component part feature)) same (configur$5 assembl$5))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/05/08 16:02

ProQuest

Basic	Advanced	Topics	Publications	🗁 My Research 0 marked items

Interface language

English ▼

Databases selected: Multiple databases...

Results

5 documents found for: *PDN(<04/10/2000) and (proxy and (referer or referrer)*   **» Refine Search | Set Up Alert** ✉
and (secure or security) and HTTP and header)

Trade Publications

🔲 Mark
all   🗁 **0** marked items: Email / Cite /
Export   📄 Show only full
text   Sort results by: Most recent first ▼

🔲   1. **None of your e-business**
        Aviel D Rubin. **Web Techniques.** Apr 2000. Vol. 5, Iss. 4; p. 55 (4 pages)

        📄 Text+Graphics   📄 Full Text - PDF   📄 Abstract

🔲   2. **Maintaining secure Web applications**
        Jeff Forristal. **Network Computing.** Manhasset: Mar 20, 2000. Vol. 11, Iss. 5; p. 93 (4 pages)

        📄 Text+Graphics   📄 Full Text - PDF   📄 Citation

🔲   3. **The Web is not TV**
        Lincoln D Stein. **Web Techniques.** Sep 1999. Vol. 4, Iss. 9; p. 18 (2 pages)

        📄 Text+Graphics   📄 Full Text - PDF   📄 Abstract

🔲   4. **How safe is the net?**
        Karen Kenworthy, Nancy A Lang, Fred Langa. **Windows Magazine.** Manhasset: Dec 1998. Vol. 9, Iss. 12;
        p. 144 (9 pages)

                                                                     📄 Citation

🔲   5. **An evaluation: Exploring Web server performance**
        Arlitt, Martin F. **Capacity Management Review.** Naples: Oct 1996. Vol. 24, Iss. 10; p. 15 (8 pages)

        📄 Text+Graphics   📄 Full Text - PDF   📄 Abstract

1-5 of 5

Want to be notified of new results for this search? Set Up Alert ✉   Results per page: 30 ▼

Basic Search

(Tools: Search Tips   Browse Topics   5 Recent Searches)

PDN(<04/10/2000) and (proxy and (referer or referrer) and (secure or securi | Search | | Clear |

Database: Multiple databases...   ▼ Select multiple databases

Date range: All dates   ▼

Limit results to: 🔲 Full text documents only 📄

                🔲 Scholarly journals, including peer-reviewed 🎓 About

L10	35	(@ad<"20000410").ad. and ((http) same secure same (box source computer machine)) and (((select$5 choos$5 determin$5 chos$5) with (component part feature)) same (configur$5 assembl$5))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/05/08 16:04
L11	38	(@ad<"20000410").ad. and ((http) same secure same (box terminal source computer machine)) and (((select$5 choos$5 determin$5 chos$5) with (component part feature)) same (configur$5 assembl$5))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/05/08 16:05
L12	17	(@ad<"20000410").ad. and ((http) same access$5 same secure same (box terminal source computer machine)) and (((select$5 choos$5 determin$5 chos$5) with (component part feature)) same (configur$5 assembl$5))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/05/08 16:07
L13	18	(@ad<"20000410").ad. and ((http) same access$5 same secure same (box terminal source computer source destination machine)) and (((select$5 choos$5 determin$5 chos$5) with (component part feature)) same (configur$5 assembl$5))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/05/08 16:07
L14	8	(@ad<"20000410").ad. and ((http) same access$5 same(source destination) same secure same (box terminal source computer machine)) and (((select$5 choos$5 determin$5 chos$5) with (component part feature)) same (configur$5 assembl$5))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/05/08 16:33
L15	2	(@ad<"20000410").ad. and (http same referrer same proxy)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/05/08 16:35
L16	139	(@ad<"20000410").ad. and (http same header same proxy)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/05/08 16:36
L17	78	(@ad<"20000410").ad. and ((http adj3 header) same proxy)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/05/08 16:36

L18	23	(@ad<"20000410").ad. and ((http adj3 header) same (proxy and url))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/05/08 16:37
L19	3	(@ad<"20000410").ad. and ((http adj3 header)) and (proxy same (physical logical) same url)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/05/08 16:39
L20	0	(@ad<"20000410").ad. and ((http adj3 header)) and (proxy same (physical logical) same url same source)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/05/08 16:40
L21	1	(@ad<"20000410").ad. and ((http adj3 header)) and (proxy same (physical logical) same source same (source URL destination))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/05/08 16:41
L22	50	(@ad<"20000410").ad. and (proxy same (physical logical) same source same (source URL destination))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/05/08 16:41
L23	14	(@ad<"20000410").ad. and (proxy same (physical logical) same source same (source URL destination)) and http	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/05/08 16:43
L24	14	(@ad<"20000410").ad. and (proxy same (physical logical) same source same (source URL destination)) and http and (known secure)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/05/08 17:13
L25	14	(@ad<"20000410").ad. and ((proxy proxies) same (physical logical) same source same (source URL destination)) and http and (known secure)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/05/08 16:44
L26	7	(@ad<"19990406").ad. and (custom or customize) and (store near5 front) and (proxy proxies)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/05/08 16:52
L27	2	(@ad<"19990406").ad. and http and (custom or customize) and (store near5 front) and (proxy proxies)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/05/08 16:53

EAST Search History

L28	2	"6,167,383".pn.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/05/08 16:52
L29	2	(@ad<"19990406").ad. and http and access$5 and (custom or customize) and (store near5 front) and (proxy proxies)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/05/08 16:54
L30	2	(@ad<"19990406").ad. and http and access$5 and (custom or customize) and (store near5 front) and (proxy proxies)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/05/08 17:13
L31	0	(@ad<"19990406").ad. and http and access$5 and (custom or customize) and (store near5 front) and (proxy proxies)	EPO; JPO; DERWENT	OR	ON	2007/05/08 17:13
L32	0	(@ad<"20000410").ad. and (proxy same (physical logical) same source same (source URL destination)) and http and (known secure)	EPO; JPO; DERWENT	OR	ON	2007/05/08 17:13
L33	0	(@ad<"20000410").ad. and (proxy and (physical logical) and source and (source URL destination)) and http and (known secure)	EPO; JPO; DERWENT	OR	ON	2007/05/08 17:14
L34	5	(@ad<"20000410").ad. and (proxy and (physical logical) and (source URL destination))	EPO; JPO; DERWENT	OR	ON	2007/05/08 17:14

DETAILED DESCRIPTION - There is an INDEPENDENT CLAIM for a computer readable code for dynamic distribution of program objects.

USE - Method is for use in moving objects dynamically from computer to computer for load balancing and clustering of objects which communicate frequently to reduce network traffic and improve overall system performance.

ADVANTAGE - Method allows dynamic reconfiguration of programs without programmer intervention, does not require modification of system program source text, and allows the administrator to specify the conditions under which reconfiguration is to occur on a per user basis.

DESCRIPTION OF DRAWING(S) - The figure shows proxy and byte code generation with

object 401

proxy generator 403

local proxy 405

remote proxy 407

byte code modifier 409

serializable object 411

ABSTRACTED-PUB-NO: US 6324543B

EQUIVALENT-ABSTRACTS:

NOVELTY - Method consists in identifying all the objects in the program, creating a list of conditions under which objects of the program are to be migrated, and identifying each programmed entity to be accessed from outside of the object. Two proxies are generated for each object, one on the same physical device and the other transferred to the remote computer on object migration. The first proxy contains network linkage and indication to access the programmed entities on the remote computers, and the second contains network linkage and indication to access the programmed entities on the first computer.

DETAILED DESCRIPTION - There is an INDEPENDENT CLAIM for a computer readable code for dynamic distribution of program objects.

USE - Method is for use in moving objects dynamically from computer to computer for load balancing and clustering of objects which communicate frequently to reduce network traffic and improve overall system performance.

ADVANTAGE - Method allows dynamic reconfiguration of programs without programmer intervention, does not require modification of system program

2

source text, and allows the administrator to specify the conditions under which reconfiguration is to occur on a per user basis.

DESCRIPTION OF DRAWING(S) - The figure shows proxy and byte code generation with

object 401

proxy generator 403

local proxy 405

remote proxy 407

byte code modifier 409

serializable object 411

CHOSEN-DRAWING:	Dwg. 4/7
TITLE-TERMS:	DYNAMIC DISTRIBUTE PROGRAM OBJECT
DERWENT-CLASS:	T01
EPI-CODES:	T01-F02C; T01-H07C5A; T01-M02A1; T01-S01B;
SECONDARY-ACC-NO:	
Non-CPI Secondary Accession Numbers:	N1999-358420

3

ProQuest

Interface language

| Basic | Advanced | Topics | Publications | 🖾 My Research
0 marked items |

English ▼

Databases selected: Multiple databases...

Document View   « Back to Results   Document 1 of 5 Next >

| Print | Email | 🖾 Mark Document   Publisher Information

None of your e-business

Aviel D Rubin. **Web Techniques**. San Francisco: Apr 2000.
Vol.5, Iss. 4; pg. 55, 4 pgs

>> **Jump to full text** 📄

>> Translate document from: Select language ▼

>> **More Like This** - Find similar documents

Other available formats:

🖾 Abstract

📄 Full Text

🗎 Full Text - PDF

Subjects:	Computer security, Electronic commerce, Information, Computer privacy
Locations:	United States, US
Author(s):	Aviel D Rubin
Document types:	Feature
Publication title:	Web Techniques. San Francisco: Apr 2000. Vol. 5, Iss. 4; pg. 55, 4 pgs
Source type:	Periodical
ISSN:	1086556X
ProQuest document ID:	50708866
Text Word Count	3189
Document URL:	http://proquest.umi.com/pqdweb?did=50708866&sid=5&Fmt=4&clientId=19649&RQT=309&VName=PQD

Abstract (Document Summary)

Online credit card information is potentially available to many people who can access it, either legitimately or otherwise, from remote locations, over networks that may or may be **secure**. Surprisingly, many people still believe that their e-mail is somewhat private. Encryption programs are a viable solution provided that they are installed by both parties. Direct compromise of privacy occurs when a company actively collects personal information, then indexes, categorizes, and shares it with people. Public humiliation is a great way to teach companies that blatantly invade people's privacy a lesson and get them to stop. Indirect methods involve compromises of privacy that are a result of a **security** incident. One way to ward off the indirect attacks described is to protect the data on a machine. People can protect their credit card numbers by refusing to enter credit card information into a Web form. There are tools for protecting browsing activity from Web servers and other users.

Full Text (3189 words)

The advent of the Internet and Its wide-scale adoption have irrevocably changed the way we interact with each other, the way we transact

business, and the way personal information is gathered and maintained about us. While progress is always exciting and provides a multitude of opportunities, there's also a dark side. Never before has there been such an opportunity for aggregating and cross-referencing personal information about people.

Before the Internet, when you physically browsed a bookstore, the store might keep track of which books you bought and which you returned. Now, you're more likely to shop online at amazon.com or barnesandnoble.com. These stores can keep track of which books you bought, which books you browsed, from which books you read a sample chapter, which books you recommended, and which books you avoided. They even know what search terms you use to locate books. Similarly, the online grocery can elicit much more information from its customers than the physical supermarket of the past, and so can the pharmacy and the online video store. In short, when you interact online, a record is created of every single action you take. But this is only half of the picture. More and more organizations are going online. So the sanctity of the sensitive records they keep is subject to the quality of their computer **security**. it doesn't do any good for an organization to maintain a respectable privacy policy if its machines are wide open to attack. Unfortunately, **security** on the web is dismal at best.

As if accidental disclosure of personal information weren't enough, there's also a huge incentive for organizations to share the information they collect. Targeted advertising is an enormous and growing market. There are companies whose sole purpose is to collect as much personal information as possible about people, cross-reference it, and sell the results to other companies.

What Is at Risk?

The privacy of many types of personal data can be compromised. Perhaps the most personal and valuable thing that you have is your identity. This includes your name, your social **security** number, and the profile kept by the organizations with which you interact. Disclosure of this data can result in theft of your identity. While this concept has been discussed hypothetically in books and movies (for example, The Net), the threat is quite real.

Other information is at risk as well. Your credit card numbers are hardly private. You give them out to the waiter at the restaurant, the telephone agent of the airline, your grocery store, and all of your online retailers. on the other hand, in all cases, these parties have an incentive to keep the credit card number to themselves. Unfortunately, it's very easy for this information to end up in the wrong hands. Online credit card information is potentially available to many people who can access it, either legitimately or otherwise, from remote locations, over networks that may or may not be **secure**. Credit card information sits in databases on computers that are often much more vulnerable than their owners realize. Recent high-profile extortion cases, where hackers demanded ransom from banks by threatening to release their customers' credit card information, demonstrate how personal information can be compromised.
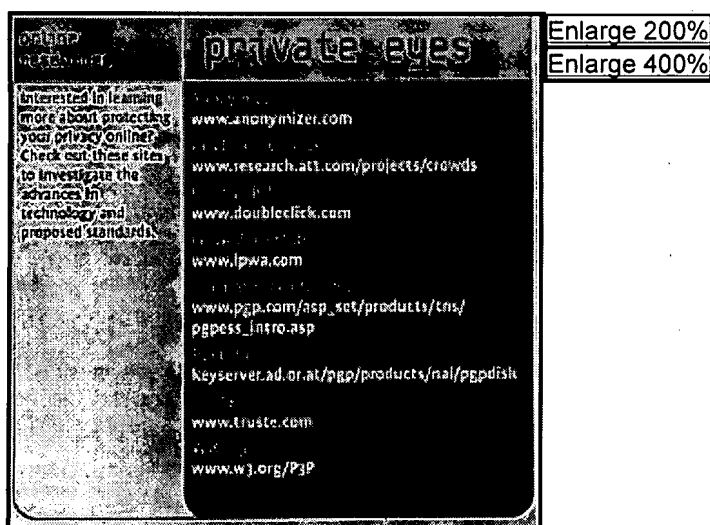
You may believe that your browsing habits-namely, which Web sites you visit, and what you do there-are private. You may believe that data on your computer is private. You may believe that the email you send is private. But all of these things are at risk on the Internet. We'll look at ways in which such private information is compromised and countermeasures that are available.

Email Privacy

With the possible exception of Web browsing, email is probably the most commonly used network application. If you're reading this magazine, you don't need to be convinced that email is as ubiquitous as the telephone. For many people, it may be even more so. if you ask most people, they'll probably tell you that their company has the ability, and in some cases the right, to read all email messages. What they probably don't realize is the extent to which email monitoring technology has advanced. Corporations can use tools to regularly monitor email for personal messages, messages that could indicate inappropriate behavior, and other information that the company could find to be of use. These tools allow sophisticated keyword searches, as well as complicated heuristics for automatically sifting through email to find whatever the authorities decide they need to find.

Surprisingly, many people still believe that their email is somewhat private. Messages are sent with personal information, ranging from gossip to performance review data, that should never be seen by other employees. Most employees don't think about the fact that not only do the system administrators have access to all email on the system, but, in many networks, so does just about everyone else.

The most common type of network in the office environment is the Ethernet. It's trivial to tap into the Internet and monitor every packet that travels on the LAN. Available programs can take the raw IP packets and reconstruct TCP streams. From there, application-level data can be assembled, and email can be monitored. Programs called sniffers can be configured easily to capture every email message that travels on an Ethernet.

Fortunately, you can take steps to counter the threats to email privacy. Unfortunately, none of the steps is that simple. The problem is that email is shared between at least two people. It doesn't make sense to protect email messages cryptographically if the recipient of your message doesn't have the ability to decrypt. Unless you two share a key, and the software to

perform encryption and decryption, your message is going to be very private-so private that even your intended recipient won't be able to read it.

Encryption programs are a viable solution provided that they're installed by both parties. One good example is PGP, which uses the RSA public key cryptosystem to provide digital signature and encryption capabilities for email. To use the system, you must first generate a key pair, using the software; the other party must do the same. Next the public keys are exported into a file, where they are manually exchanged by both parties. "Manually" means that you shouldn't use an untrusted network to exchange the keys. The best way to exchange them is in person. If this isn't practical, you can exchange the public keys over an insecure network, but after doing so, verify the built-in fingerprint of each key with each other by phone. The fingerprint is simply the MD5 hash of the bits of the public key, in hex format. MD5 is a cryptographic checksum function that is used to detect data tampering.

Once you have each other's public keys, you can use the PGP software to encrypt and/or sign a message. On the other end, the software can bi used to decrypt and/or verify signatures, depending on the option chosen by the sender.

PGP is just one option. Another solution that also uses the RSA cryptosystem has been standardized by the Internet Engineering Task Force (IETF). This is called S/MIME, and it's convenient in that it's nicely integrated into the commonly used Microsoft Outlook and Netscape Messenger mail programs. To use S/MIME, you must first generate a key pair and obtain a certificate for your public key. The good thing about a standard is that the software for using it is available in many different browsers. The browsers also contain root public keys that can be used to verify a certificate, regardless of which certifying authority signs it.

The main difference between PGP and S/MIME is that in the former, users are responsible for distributing their public keys to one another. on the other hand, in S/MIME, certifying authorities act as introducers for people, and as long as everyone shares a common set of root public keys, the authentication system works. PGP is more appropriate for a diverse set of people with no common authority. S/MIME is geared toward organizations with tight hierarchical structures.

Other systems, such as Lotus Notes, operate similarly to S/MIME. However, users should be careful when using a mail system in which the cryptography is administered by their own organization. It's possible, even likely, that management has a way of bypassing the cryptography to get at the messages. This can be accomplished by making extra copies of private keys, or by using functions with back doors.

How Is Personal Privacy Compromised?

Whether you're concerned with email privacy, confidentiality of credit card numbers, or protecting your browsing history, you need to understand how the risks manifest themselves directly and indirectly. Direct methods are those that result in loss of privacy due to action on the part of the parties with whom you interact and their partners. Indirect methods are ways in which privacy can be lost despite the best behavior of the parties involved.

The Direct Approach

Direct compromise of privacy occurs when a company actively collects your

personal information, then indexes, categorizes, and shares it with people. This has been going on for a long time. Personal information about you is so valuable that many organizations offer free or discount services in exchange for this information. The Web is an ideal platform for companies that operate in this space. Take DoubleClick, for example. it stores ads on Web pages and then uses cookies to correlate requests across Web sessions.

Enlarge 200%
Enlarge 400%

Enlarge 200%
Enlarge 400%
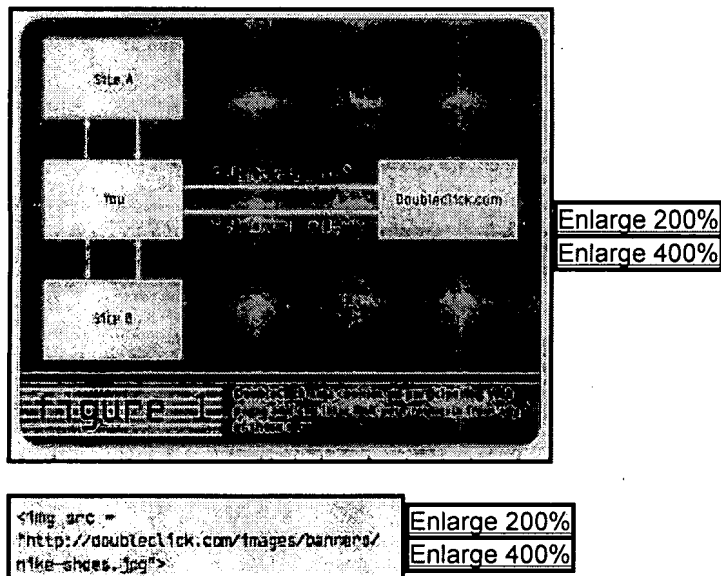
Figure 1 illustrates how this works. You, the innocent user, visit site A. in doing so, you download a Web page from the site. The Web page that you download has, among other things, an image that resides on DoubleClick.com's Web site. For example, the following HTML segment

Enlarge 200%
Enlarge 400%

causes your browser to fetch the image nike-shoes.jpg from the DoubleClick site. When DoubleClick serves the page, it also includes a cookie in the response. This is just a **header** of the format:

Upon receiving this, your browser displays the image, and stores the cookie value in the cookie file on your local disk.

At some point in the future, you visit site B. This site is also a customer of DoubleClick's. When your browser loads site B's Web page, it contains an embedded image from DoubleClick. When the page loads, your browser requests the image. However, since your cookie file contains a cookie that was set by DoubleClick, the cookie is returned as well. Thus, DoubleClick can correlate that the request from site A and the request from site B came from the same browser. As a result, DoubleClick can build a whole list of sites that a particular user visits. This is due to a special **HTTP header** called the **Referer** field. The **Referer** head relays to DoubleClick the URL of the page that the user requested from site A or B. Consider the implications of this. Many search engine requests include the search terms in the URL. In fact, when search values are sent to a CGI script on a server using the GET method, the fields filled in by the user are all included in the URL. This gives DoubleClick all sorts of valuable information, which can be mined by powerful algorithms and offered for sale to the highest bidder. For example, a company that determines whether to approve someone for health

insurance might be interested in this information.

Another example of surreptitious use of the direct method involves RealNetworks. This company provides streaming video and audio through Web browsers. After it was in business for some time, an independent **security** expert, Richard Smith, discovered that the RealNetworks software collected information from peoples' browserswithout their permission-about the content that users requested. This invasion of privacy was halted when stories in the media proved a big slap in the face to the company. Public humiliation is a great way to teach companies that blatantly invade your privacy a lesson, and more importantly, to get them to stop.

Covert Operations

Indirect methods involve compromises of privacy that are a result of a **security** incident. For example, a malicious worm can propagate quickly across the Internet. Worms such as Melissa, Explorer.zip, and friends may have been infuriating, but as far as we know, they weren't attacks against privacy. It isn't too difficult to envision a malicious version of a worm that secretly searches a computer for "interesting" looking content and covertly discloses it to a remote location. While we haven't seen such a thing on a broad scale, these types of malicious programs could be a very real danger in the near future.

OK, enough gloom and doom. what can you do to protect yourself? We'll examine some defense mechanisms you can use to try to win back some of your privacy.

Protect Data an Your Machine

One way to ward off the indirect attacks described is to protect the data on your machine. You want to protect the information for the worstcase scenario-such as when a perpetrator runs arbitrary programs, like an Internet worm/virus, right on your computer. The only way to properly achieve this is with cryptography. There are programs available for encrypting the information on your hard drive. A great one is PGPDisk, which lets you mount an encrypted drive. The data is encrypted with a key derived from a user-supplied passphrase. When the drive is mounted, all of the data is decrypted as it is read from disk and encrypted as it is written to disk. When the drive isn't mounted, the data is available only in encrypted form, and the key is removed from memory. The privacy of your information is preserved because an intruder has no way of reading your files.

Protect Credit Card Information

Credit card information is the most widely used personal data that users readily provide to Web servers. Recent cases of extortion demonstrate that lists of credit card numbers are very valuable to merchants, advertisers, the owners of the cards, and, probably most of all, the credit card companies. The inherent insecurity of the Internet makes it relatively easy for a determined attacker to steal credit card numbers. What can you do to protect your credit card numbers? There are several approaches.

The first thing you can do is refuse to enter your credit card information into a Web form. While this may seem drastic at first, you can be assured that most Web merchants offer a mechanism for you to provide the payment information by telephone or mail. Keep in mind that the only insecure link that you avoid by doing this is the connection from your computer to the server. All of the back-end processes on the server will still contain your

information as soon as you speak it into the phone.

If you're a bit more intrepid, enter your credit card number into a Web form. But first, check to make sure that you're communicating over a **secure** channel that uses SSL. Look for a closed lock on the browser and make sure that the URL is of the form **https**:// as opposed to **http**://. Once you know that you're using SSL, you can be pretty confident that the session is encrypted. To avoid poor encryption, you should examine your **security** preferences in the browser and turn off SSL version 2, as well as all of the ciphersuites that use 56-bit encryption or less. Next, it's important to verify that your machine is speaking with the right server and not an imposter that's trying to get at your personal information. To verify this, before you enter your credit card number, check that the certificate is signed by an authority that you know and trust, and that the certified entity in the certificate is the one that you want to provide with your credit card number. Finally, pay attention to any warnings that the browser pops up at you.

Although your personal liability is probably limited to $50 in case of credit card fraud, remember that other kinds of misuse of your private information may go unnoticed for a while. It's important to be very careful when using "**secure**" Web sites. Keep in mind that even if the channel from you to the merchant is **secure**, you have almost no way of knowing how carefully the merchant's computers are monitored.

One final word on protecting credit card information. Check whether the sites with which you shop offer a privacy policy. Read the policy and make sure that you're willing to accept the terms listed. There are privacy sea] programs, such as TrustE, that audit sites to make sure they're complying with their stated policies. If you believe that they're doing a good job, it may give you reason to have more confidence in a privacy policy. Finally, a more long-term effort is underway at the W3C consortium. A project called P3P is designed to allow users and Web sites to automatically negotiate a level of privacy protection for information. (For more information, see the article "Privacy Critics," Web Techniques, September 1999.)

Safeguard Your History

There are several ways that your browser keeps track of your online browsing habits. The browser history shows past URLs you've requested. In Netscape Navigator, the prefs.js file keeps a list of URLs you entered into the location window. Also, the local cache keeps copies of things you browse. if you share your computer with others, it's a good idea to clear all of these if you care to protect your privacy regarding the sites that you browse.

There are also tools for protecting your browsing activity from Web servers and other users. AT&T Labs Crowds is a system for browsing the Web in such a way that others can't tell that it's you browsing. To use the system, you join a crowd of other users by running a **proxy** on your machine. From then on, your actions are indistinguishable from those of others in the crowd. Another option called Anonymizer is a commercial system that hides your location from end servers. However, the administrators of the Anonymizer themselves can collect the information. Another system, ProxyMate, can be used for Web sites that require subscription services. ProxyMate provides you with pseudonyms and remembers passwords for you. The names and passwords are generated randomly, so that Web sites can't link your activity to a real-world person based on the information you enter.

Summary

In our world of ever-advancing technology, privacy has become a casualty. As more of our daily activities, interests, and relationships move onto computers, the potential for misuse of this information increases. Web server logs do not forget, and the technology for correlating information and building up data shadows about people is constantly improving. The technologies are in their infancy, and the ability to compromise privacy is growing faster than our ability to protect ourselves. Without a focused research effort on privacy technologies, and perhaps legislation, the future may be a much darker place. :0-C

[Author Affiliation]

More Like This - Find similar documents

Subjects: ▣ Computer **security** ▣ Electronic commerce
                   ▣ Information ▣ Computer privacy

Locations: ▣ United States ▣ US

Author(s):   ▣ Aviel D Rubin

Document types: ▣ Feature

Language: ▣ English

Publication title: ▣ Web Techniques

| Search | | Clear |

| Print | | Email | ▣ Mark Document   Publisher Information

---

^ Back to Top   ‹‹ Back to Results   Document 1 of 5 Next >

ProQuest CSA

ProQuest

Basic	Advanced	Topics	Publications	My Research 0 marked items

Interface language

English ▼

Databases selected: Multiple databases...

Results – powered by ProQuest® Smart Search

Suggested Topics   About   < Pr

Securities regulations AND Proxies

150 documents found for: *PDN(<04/10/2000) and (proxy and (secure or security) and HTTP and header)*   » **Refine Search | Set Up Alert** ✉

All sources	🎓 Scholarly Journals	Magazines	Trade Publications	Newspapers

🖾 Mark all   📂 **0** marked items: Email / Cite / Export   📄 **Show only full text**   Sort results by: Most r

---

1. **Turn a Solaris box into a packet-filtering firewall**
   Boris Loza. **Inside Solaris.** Louisville: Apr 2000. Vol. 6, Iss. 4; p. 1 (6 pages)

   📄 Text+Graphics   📄 Full Text - PDF   📄 Abstract

---

2. **Commercialization of electronic information**
   Jean-Henry Morin, Dimitri Konstantas. **Journal of End User Computing.** Apr-Jun 2000. Vol. 12, Iss. 2; p.

   📄 Text+Graphics   📄 Full Text - PDF   📄 Abstract

---

3. **None of your e-business**
   Aviel D Rubin. **Web Techniques.** Apr 2000. Vol. 5, Iss. 4; p. 55 (4 pages)

   📄 Text+Graphics   📄 Full Text - PDF   📄 Abstract

---

4. **Maintaining secure Web applications**
   Jeff Forristal. **Network Computing.** Manhasset: Mar 20, 2000. Vol. 11, Iss. 5; p. 93 (4 pages)

   📄 Text+Graphics   📄 Full Text - PDF   📄 Citation

---

5. **A Framework and Lightweight Protocol for Multimedia Network Management**
   Jairo A. Gutierrez, Donald P. Sheridan, R. Radhakrishna Pillai. **Journal of Network and Systems Manage**
   York: Mar 2000. Vol. 8, Iss. 1; p. 33

   📄 Article image - PDF   📄 Abstract

---

6. **Caching in with content delivery**
   Jonathan Angel. **Network Magazine.** Mar 2000. Vol. 15, Iss. 3; p. 92 (5 pages)

   📄 Text+Graphics   📄 Full Text - PDF   📄 Abstract

---

7. **Turnkey solutions meet Web demands**
   Ian Agranat, Daryl Rudusky. **Electronic Engineering Times.** Manhasset: Feb 28, 2000. ; p. 106 (4 pages)

   📄 Text+Graphics   📄 Full Text - PDF   📄 Citation

---

8. **'Cookie cutting' keeps traffic moving**
   Ted Schroeder. **Network World.** Framingham: Feb 21, 2000. Vol. 17, Iss. 8; p. 49 (1 page)

   📄 Text+Graphics   📄 Full Text - PDF   📄 Abstract

---

9. <u>IO-Lite; a unified I/O buffering and caching system</u>
   Vivek S. Pai, Peter Druschel, Willy Zwaenepoel. **ACM Transactions on Computer Systems.** New York: F
   18, Iss. 1; p. 37

   🗗 Link to full text   🖽 Abstract

10. <u>My agent will call your agent</u>
    Martin L Griss. **Software Development.** San Francisco: Feb 2000. Vol. 8, Iss. 2; p. 43 (4 pages)

                                                                 🖽 Abstract

11. <u>IP challenges QoS requirements</u>
    Azhar Sayeed. **Electronic Engineering Times.** Manhasset: Jan 24, 2000. ; p. 110 (4 pages)

    🖺 Text+Graphics   🔁 Full Text - PDF   🖽 Citation

12. <u>Web traffic complexitites change LANscape</u>
    Loring Wirbel. **Electronic Engineering Times.** Manhasset: Jan 24, 2000. ; p. 93 (2 pages)

    🖺 Text+Graphics   🔁 Full Text - PDF   🖽 Citation

13. <u>FIREWALLS 101: THREE COMMON PROTECTION SCHEMES; [ONLINE Edition]</u>
    Troy Denkinger Special to the Tribune. **Chicago Tribune.** Chicago, Ill.: Jan 13, 2000. ; p. 1

    🖹 Full text   🖽 Abstract

14. <u>SSL and TLS protocols: How to address critical security issues</u>
    Rolf Oppliger. **Computer Security Journal.** San Francisco: Winter 2000. Vol. 16, Iss. 1; p. 15 (24 pages)

                                                                 🖽 Abstract

15. <u>Emulator express: A system for optimizing emulator performance for wireless networks</u>
    B C Housel, I Shields. **IBM.Systems Journal.** Armonk: 2000. Vol. 39, Iss. 2; p. 384 (19 pages)

    🖺 Text+Graphics   🔁 Full Text - PDF   🖽 Abstract

16. <u>A model for library support of distance education in the USA</u>
    Jean L.Cooper. **Interlending & Document Supply.** Bradford: 2000. Vol. 28, Iss. 3; p. 123

    🖹 Full text   🖽 Abstract

17. <u>Interlending and document supply: a review of recent literature XXXVIII</u>
    Sara Gould. **Interlending & Document Supply.** Bradford: 2000. Vol. 28, Iss. 3; p. 143

    🖹 Full text   🖽 Abstract

18. <u>Wireless Access Protocol set to take over; WAP addresses the shortcomings of other protocols</u>
    Rawn Shah. **JavaWorld.** San Francisco: Jan 1, 2000. ; p. 1

    🖹 Full text   🖽 Abstract

19. <u>Bobby: An online tool for Web site designers</u>
    Jessica Chaiken, David Johnson. **Library Hi Tech News.** Bradford: 2000. Vol. 17, Iss. 2; p. 28 (4 pages)

    🖺 Text+Graphics   🔁 Full Text - PDF   🖽 Abstract

20. <u>Active directory doesn't just manage network resources, it can manage your data too</u>
    Shawn Wildermuth. **Microsoft Systems Journal.** San Francisco: Jan 2000. Vol. 15, Iss. 1; p. 51 (14 page:

                                                                 🖽 Abstract

21. <u>On proxy agents, mobility, and web access</u>
    Anupam Joshi. **Mobile Networks and Applications.** Amsterdam: 2000. Vol. 5, Iss. 4; p. 233

    🔁 Article image - PDF   🖽 Abstract

22. **The Satchel system architecture: Mobile access to documents and services**
Mike Flynn, David Pendlebury, Chris Jones, Marge Eldridge, Mik Lamming. **Mobile Networks and Applica**
Amsterdam: 2000. Vol. 5, Iss. 4; p. 243

      📄 Article image - PDF   📧 Abstract

23. **Optimizing Internet bandwidth**
Ralph Barker. **Performance Computing.** San Francisco: Jan 2000. Vol. 18, Iss. 2; p. 29 (5 pages)

      📄 Text+Graphics   📄 Full Text - PDF   📧 Abstract

24. **Sites Strive To Hold On To Buyers**
Christine Zimmerman. **InternetWeek.** Manhasset: Nov 29, 1999. ; p. PG.1

      📄 Full text   📧 Abstract

25. **The Iceberg Project: Defining the IP and Telecom Intersection**
Bhaskaran Raman, Helen J. Wang, Jimmy Shih, Anthony D. Joseph, Randy H. Katz. **IT Professional Mag**
Washington: Nov/Dec 1999. Vol. 1, Iss. 6; p. 38

      📄 Full Text - PDF   📧 Abstract

26. **ASIS mid-year 1999: Evaluating and using networked information resources and services**
Arthur Hendricks. **Library Hi Tech News.** Bradford: Nov 1999. ; p. 9 (6 pages)

      📄 Full text   📄 Full Text - PDF   📧 Abstract

27. **Intrusion detection systems: Expectations, ideals and realities**
Marcus Ranum. **Computer Security Journal.** San Francisco: Fall 1999. Vol. 15, Iss. 4; p. 25 (21 pages)

                                     📧 Abstract

28. **The QoS quagmire**
Tom Stenson. **Network World.** Framingham: Sep 6, 1999. Vol. 16, Iss. 36; p. 53 (3 pages)

      📄 Text+Graphics   📄 Full Text - PDF   📧 Abstract

29. **WAP: New Web whopper**
Joshua Piven. **Computer Technology Review.** Los Angeles: Sep 1999. Vol. 19, Iss. 9; p. 1 (3 pages)

      📄 Text+Graphics   📄 Full Text - PDF   📧 Abstract

30. **Video servers revisited**
Jonathan Angel. **Network Magazine.** Sep 1999. Vol. 14, Iss. 9; p. 56 (5 pages)

      📄 Text+Graphics   📄 Full Text - PDF   📧 Abstract

1-30 of 150   < First | < Previous 1 2

Want to be notified of new results for this search? Set Up Alert ✉   Results p

Did you find what you're looking for? If not, **refine your search** below or try these suggestions.

    Suggested Topics About   < Pr

    Securities regulations AND Proxies

△**Tools:**   Search Tips   Browse Topics   2 Recent Searches ▷

Basic Search

| PDN(<04/10/2000) and (proxy and (secure or security) and HTTP and heade | **Search** | **Clear** |

Database: Multiple databases...   ▼ <u>Select multiple databases</u>

Date range: All dates   ▼

Limit results to: ▣ Full text documents only 📄

              ▣ Scholarly journals, including peer-reviewed 🎓 <u>About</u>

〔More Search Options〕 ∧ <u>Hide options</u>

Publication title: [   ]   <u>Browse publications</u> <u>About</u>

Author: [   ]   <u>About</u>

Look for terms in: Citation and document text   ▼ <u>About</u>

Document type: Any document type   ▼

Publication type: All publication types   ▼

Exclude from results: ▣ Book Reviews

                 ▣ Dissertations

                 ▣ Newspapers

Sort results by: Most recent first   ▼

ProQuest CSA